1. Группа, подгруппа. Простейшие свойства.

Определение

Пусть G — множество, и определена $\cdot : G \times G \to G$, удовлетворяющая следующим условиям.

1) *Ассоциативность* $\forall a, b, c \in G \quad (ab)c = a(bc)$.

2) *Нейтральный элемент.* $\exists e \in G$ такой, что $\forall a \in G \quad ae = ea = a$.

3) *Обратный элемент.* $\forall a \in G \ \exists a^{-1} \in G$ такой, что $a \cdot a^{-1} = a^{-1} \cdot a = e$.

4) *Коммутативность* $\forall a, b \in G \quad ab = ba$.

- Если выполнены условия 1 и 2, то G — *полугруппа*.
- Если выполнены условия 1, 2 и 3, то G — *группа*.
- Если выполнены условия 1, 2, 3 и 4, то G — *абелева группа* (или, что то же самое, *коммутативная группа*).
- Операцию в группе можно обозначать как угодно, как правило, используется символ $\cdot$, но это не обязательно.

Определение

Если G и H — группы с одинаковой операцией $\cdot$ и $H \subset G$, то H — *подгруппа* G. Обозначение: $H < G$.

Свойство 1

Нейтральный элемент единственен

Доказательство. Пусть их два: e_1 и e_2. Тогда $e_1 = e_1 e_2 = e_2$. □

Свойство 2

Для любого $a \in G$, обратный элемент a^{-1} единственен.

Доказательство. Пусть a_1 и a_2 — два обратных элемента к $a \in G$. Тогда $a_1 a = a a_2 = e$, откуда $a_1 = a_1(a a_2) = (a_1 a) a_2 = a_2$. □

Свойство 3

Для любого $a \in G$, $(a^{-1})^{-1} = a$.

Доказательство. Так как $a a^{-1} = a^{-1} a = e$, значит, a является обратным к a^{-1}. По Свойству 2, обратный элемент единственен. □

Свойство 4

Для любых $a, b \in G$ выполнено $(ab)^{-1} = b^{-1} a^{-1}$.

Доказательство. $b^{-1} a^{-1} ab = abb^{-1} a^{-1} = e$. □

Лемма 1

Пусть G — группа, $H \subset G$, причем H замкнуто по умножению и взятию обратного элемента (то есть, $\forall a, b \in H$ выполнено $ab \in H$ и $a^{-1} \in H$). Тогда $H < G$.

Доказательство. • При выполнении этих условий, $\cdot : H \times H \to H$ — ассоциативная операция и для любого элемента существует обратный.

• Пусть $a \in H$. Тогда $a^{-1} \in H \Rightarrow e = aa^{-1} \in H$.

• Значит, H — группа с операцией $\cdot$, то есть, $H < G$. □

Лемма 2

Пусть $\{H_i\}_{i \in I}$ — множество подгрупп группы G. Тогда $H = \bigcap\limits_{i \in I} H_i$ — тоже подгруппа группы G.

Доказательство. • Достаточно проверить замкнутость по умножению и взятию обратного элемента.

• Пусть $a, b \in H$. Тогда для всех $i \in I$ мы имеем $a, b \in H_i$.

• Следовательно, для всех $i \in I$ мы имеем $ab \in H_i$, откуда следует, что $ab \in H$.

• Кроме того, для всех $i \in I$ мы имеем $a^{-1} \in H_i$, откуда следует, что $a^{-1} \in H$. □

2. Подгруппа, порожденная множеством элементов

Подгруппа, порожденная множеством элементов

Определение

Пусть G — группа, $M \subset G$. Тогда

$\langle M \rangle := \{ t_1 \dots t_n \ : \ \forall i \in \{1, \dots, n\} \ t_i \in M \text{ или } t_i^{-1} \in M. \}$

(n не фиксировано, может быть любым натуральным числом)

— *подгруппа, порожденная M*.

Лемма 3

Пусть G — группа, $M \subset G$. Тогда $\langle M \rangle < G$.

Доказательство. • Поскольку группа G замкнута по умножению и взятию обратных элементов, $\langle M \rangle \subset G$. (Из $t_i^{-1} \in M \subset G$ следует $t_i = (t_i^{-1})^{-1} \in G$. Из $t_1, \dots, t_n \in G$ следует $t = t_1 \dots t_n \in G$.

• Пусть $t, s \in \langle M \rangle$. Тогда $t = t_1 \dots t_n$ (где $t_i \in M$ или $t_i^{-1} \in M$ для всех i) и $s = s_1 \dots s_m$ (где $s_i \in M$ или $s_i^{-1} \in M$ для всех i).

• Тогда $ts = t_1 \dots t_n s_1 \dots s_m \in \langle M \rangle$.

• $t^{-1} = t_n^{-1} \cdot \dots \cdot t_1^{-1} \in \langle M \rangle$, так как для любого i либо $t_i^{-1} \in M$, либо $(t_i^{-1})^{-1} = t_i \in M$.

• По Лемме 1, $\langle M \rangle < G$. □